PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-057554
(43)Date of publication of application : 27.02.2001

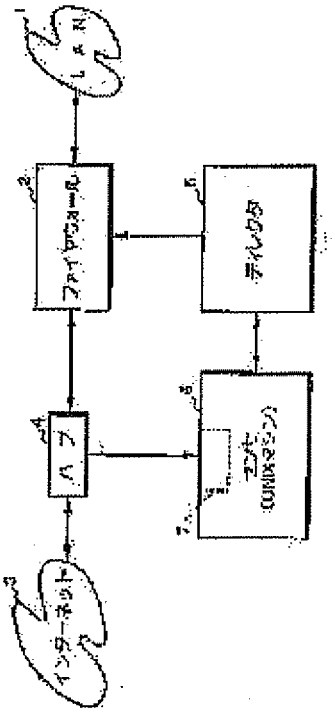
(51)Int.Cl. H04L 12/24
H04L 12/26
H04L 12/46
H04L 12/28
H04L 12/66
H04L 12/56

(21)Application number : 11-265942
(22)Date of filing : 17.08.1999

(71)Applicant : BABA YOSHIMI
(72)Inventor : BABA YOSHIMI

(54) CRACKER MONITOR SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a cracker monitor system that can automatically detect an attack from a cracker on a network and protect the network from the attack by the cracker in spite of a simple system configuration without limiting the communication as required or over and the need for a labor by a skillful engineer.
SOLUTION: An entrance of a LAN 1 is provided with a sensor 5 that sequentially acquires an IP packet passing through the entrance. The sensor 5 senses various attacks from a cracker with respect to the LAN 1 on the basis of the acquired IP packet. Information with respect to the attacker sensed by the sensor 5 is given to a director 6 controlling a firewall 2. The director 6 controls the setting of the firewall 2 in response to the given information to block the IP packet relating to the sensed attack from entering the LAN 1.



(Partial Translation)

JP 2001-057554 A

[Embodiment of the invention]

[0008] An embodiment according to the present invention is explained with reference to Fig. 1. Fig. 1 is a diagram of a system configuration according to the present embodiment. In Fig. 1, numeral 1 is a LAN as a network. The LAN 1 is architectured with, for example, Ethernet, and a plurality of hosts (computers) (not shown) are connected via an Ethernet cable, hub, and the like. An Ethernet card for connecting to the Ethernet cable, software for performing TCP/IP processing, various application software that run on the TCP/IP (for example, telnet, ftp, and smtp) are implemented in each of the hosts, enabling communication based upon the IP. The LAN 1 is not limited to the architectured network on the Ethernet, however any architecture mode such as token ring and the like can be employed. In the system according to the present embodiment, a computer 2 having a function of a firewall as a packet filter (hereinafter, simply "firewall 2 for the computer 2") is arranged at an entrance for the LAN1. The LAN1 is connected to an internet 3 via the firewall 2. The firewall 2 has a file (hereinafter, "filter setting file") in which data is written for defining what type of IP packet is prohibited for entering into the LAN 1. When the type of the IP packet that is prohibited for entering into the LAN 1 is sent from a side of the internet 3 by the filter setting file, the IP packet is discarded to block the entry into the LAN 1. When the IP packet that is not prohibited for entering into the LAN 1 is sent by the filter setting file, the IP packet is transferred to the LAN 1. A hub 4 is mounted between the firewall 2 and the

internet 3, and a sensor 5 having a function as an attack detecting unit is connected to the hub 4. Furthermore, a director 6 having a function as a processing unit that controls the firewall 2 is connected to the sensor 5. The sensor 5 and the director 6 are respectively configured with a computer. The sensor 5 is, for example, configured with an NIX machine and connected to the hub 4 via the Ethernet card 7. In this case, software called TCP DUMP is implemented in the sensor 5. The TCP DUMP enables acquiring (hearing) all IP packets that pass through the hub 4 via the Ethernet card 7. The sensor 5 stores and retains each of the acquired IP packets and the time data indicative of time at which the IP packet is acquired in hard disk (not shown). If the total number of the IP packets stored in the hard disk reaches the predetermined allowable capacity, the sensor 5 deletes the oldest IP packet to store newly acquired IP packet in the hard disk. Furthermore, the sensor 5 does not have an IP address and can receive (load) only the IP packet by setting the software not to be responsive to the response-requesting packet to be sent such as ARP (Address ResolutionProtocol), RARP (Reverse AdressResolution Protocol), and the like. Moreover, software (hereinafter, "attack detecting algorithm) for detecting the first to sixth type attacks mentioned above are implemented in the sensor 5. The attack detecting algorithm can be implemented in the director 6 allowing the sensor 5 to perform processing the attack detecting algorithm while sending and receiving date to and from the director 6. Software (hereinafter, "filter control algorithm) that controls the firewall 2 is implemented in the director 6. In this case, the filter control algorithm rewrites the date of the filter setting file depending upon the attack detected by the sensor 5 to control the firewall 2. Next, operation according to the

present embodiment is explained. The sensor 5 performs the following processing per predetermined cycle time while storing the acquired IP packet in the hard disk. That is, a plurality of the IP packets for the predetermined time interval are classified (sorted) per value of source IP address and value of destination IP address to be loaded into a memory (not shown). In other words, out of the IP packets for the predetermined time interval, the IP packets having the identical source IP address are consolidated and the IP packets having the identical destination IP address are consolidated to be loaded into the memory (hereinafter, a consolidated set of the IP packets is referred to as "IP packet group"). A plurality of the IP packets loaded into the memory are processed for attack detection that is mentioned later and then the IP packets are deleted from the memory. In this case, the IP packets to be loaded into the memory are IP packets that are acquired after predetermined time elapses since acquiring the oldest IP packet in the IP packets loaded into the memory in the previous cycle time. The processing for attack detection by the sensor 5 in each cycle time is performed in the following manner based upon the attack detection algorithm. The sensor 5 processes detecting, for example, the first type attack out of the first to sixth attacks, namely port scanning. In this processing, for each IP packet group that has the identical source IP address and the source IP address is for an external from the LAN 1 in the IP packets loaded into the memory as described above, the sensor 5 extracts value (IP address value belonging to LAN 1) for all the destination IP addresses held by the IP packets that are included in the each IP packet group. Thereafter, for each value for the destination IP address extracted in the above each IP packet group, the sensor 5 counts the number of the IP packets that are acquired in predetermined

continuous time (for example, within 30 seconds), and that have the identical destination IP address to the value for the above destination IP address from the IP packet group (IP packet group of the identical source IP address) having different destination port number in the TCP header or the UDP header. When the counted number reaches the predetermined number (for example, 20), the sensor 5 detects attacking of port scanning and sends the data indicative of the attack together with value data (hereinafter, "first type attack detection data") for the source IP address of the IP packet group on which the attack is detected to the director 6. Such processing is performed sequentially for all IP packet groups having the identical source IP address that does not belong to LAN 1. In the present embodiment, detection of port scanning is performed by counting the number of the IP packets having different port numbers, however the detection of port scanning can be performed by the following processing. Namely, for each IP packet group having the identical source IP address and the source IP address is for an external from the LAN 1, by extracting value for all the destination port numbers held by the IP packets that are included in the each IP packet group, the number of the IP packets that are acquired within predetermined continuous time and that have the identical destination port number to the value for the above destination port number and have different destination IP addresses is counted from the IP packet group with the extracted destination port number with respective to each value of the extracted destination port number. When the counted number reaches the predetermined number, port scanning is detected. On the other hand, the director 6 that is provided with the first type attack detection data from the sensor 5 rewrites the filter setting file of the firewall 2 to block the entry of

the IP packets that have the identical source IP address to the source IP address included in the first type attack detection data for predetermined time (for example, for five minutes) from the present time. In this time, upon receiving the IP packets having the source IP address from the internet 3, the firewall 2 discards the IP packets to block the entry thereof into the LAN 1, whereby the LAN 1 is protected from the attack of port scanning. If the director 6 is again provided with the first type attack detection data identical to the first type attack detection data that is previously provided before predetermined time (five minutes) elapses, the director 6 controls the firewall 2 to block the entry of the IP packets from the source IP address of the first type attack detection data into the LAN 1. Accordingly, unless attacking of port scanning continues, the IP packets from the source IP address cannot enter into the LAN 1. If the director 6 is not provided with the first type attack detection data again within the predetermined time (five minutes), blocking of the entry into the LAN 1 by the IP packets from the IP source address of the first type attack detection data is released. In this manner, after the sensor 5 completes processing for detecting an attack of port scanning, the sensor 5 performs processing for second type attack detection (SYN FLOOD). In this processing, for the IP groups having the identical destination IP address, the sensor 5 sequentially extracts the IP packets for SYN included in the each IP packet group having the destination IP address that belongs to LAN 1 in chronological order of acquiring thereof. Thereafter, the sensor 5 checks whether the IP packets for SYN acquired within predetermined time (for example, 2 seconds) from the time acquiring the extracted IP packets for each SYN present in the IP packet group having the identical destination address. In case of

presence, the sensor 5 counts the number of the IP packets for SYN including the previously extracted IP packets for SYN. Moreover, for the counted IP packets for SYN, the sensor 5 checks whether the IP packets for ACK corresponding to respective IP packets for SYN (IP packets for ACK having the identical source IP address to that for the IP packets for the SNY, and having the next sequence number to the sequence number in the TCP header for the IP packets for the SYN) that are acquired within the predetermined time (2 seconds) from the time for acquiring the IP packets for the SYN present in the IP packet group having the identical destination address. In case of presence, the number of the counts is decremented by one for every time. If the count is equal to or greater than the predetermined number (for example, 16) at the time of finally completing checking of the presence of the corresponding IP packets for ACK, an attack of SYN FOOD is detected and the data indicative of such attack and the value data for the source IP address and the value data for the destination IP address (hereinafter, "second type attack detection data") of the IP packets for SYN for which the attack is detected are provided to the director 6. Such processing is performed sequentially for all IP packet groups having the identical destination IP address that belongs to LAN 1. In the present embodiment, detection of SYN FLOOD is performed based upon the number of the IP packets for SYN, however the detection of SYN FLOOD can be performed by the following processing. Namely, for each IP packet group having the identical source IP address that belongs to the LAN 1, IP packets for SYN/ACK included in the IP packet group are extracted in chronological order of acquiring thereof. Thereafter, the sensor 5 checks whether the IP packets for SYN/ACK acquired within the predetermined time (for example, 2 seconds) from the time

of acquiring the extracted IP packets for each SYN/ACK present in the IP packet group having the identical source address. In case of presence, the sensor 5 counts the number of the IP packets for SYN/ACK including the previously extracted IP packets for SYN/ACK. Moreover, for the respective IP packets for SYN/ACK, the sensor 5 checks the IP packet group having the identical destination address to that for the source IP address for presence of the IP packets for ACK corresponding to the IP packets for the SYN/ACK (IP packets or ACK having the identical destination IP address to the source address for the IP packets for the SYN/ACK, and having the next ACK number to the sequence number in the TCP header for the IP packets for the SYN/ACK) that are acquired within the predetermined time (2 seconds) from the time for acquiring the IP packets for the SYN/ACK present in the IP packet group. If such packets for ACK present, the number of the counts is decremented by one for every time. If the count is equal to or greater than the predetermined number (for example, 16) at the time of finally completing checking of the presence of the corresponding IP packets for ACK, an attack of SYN FOOD is detected. In this case, the data to be provided to the director 6 form the sensor 5 are the data indicative of detection of the attack of SYN FOOD, the value data for the source IP address and the value data for the destination IP address of the IP packets for the SYN/ACK. In this case, the value data for the source IP address and the value data for the destination IP address of the IP packets for SYN/ACK respectively correspond to the value data for the source IP address and the value data for the destination IP address of the IP packets for SYN in the aforementioned second type attack detection data. The director 6 that is provided with the second type attack detection data from the sensor 5 rewrites the filter

setting file of the firewall 2 to block the entry of the IP packets having the identical source IP address to the source IP address included in the second type attack detection data for predetermined time (for example, for two minutes) from the present time. Simultaneously, the director 6 rewrites the filter setting file of the firewall 2 to block the entry of the IP packets having the identical destination IP address to the destination IP address included in the second type attack detection data for predetermined time (for example, for two minutes) from the present time. In this time, upon receiving the IP packets having the source IP address or the IP packets having the destination IP address from the internet 3, the firewall 2 discards the IP packets to block the entry thereof into the LAN 1, whereby the LAN 1 is protected from the attack of SYN FLOOD and the host having the attacking target IP address can be resumed to the normal state without shutting down. Similarly to the case for detecting port scanning, if the director 6 is again provided by the sensor 5 with the second type attack detection data identical to the second type attack detection data that is previously provided before predetermined time (two minutes) elapses for eliminating the IP packets having the source IP address in the second type attack detection data, the director 6 controls the firewall 2 to block the entry of the IP packets from the source IP address of the second type attack detection data into the LAN 1. The same can be applied to elimination of the IP packets having the destination IP address in the second type attack detection data. Accordingly, unless attacking of SYN FLOOD continues, the IP packets from the source IP address associated with the attack or the IP packets from the destination IP address associated with the attack cannot enter into the LAN 1. For elimination of any one of the IP packets having

the source IP address in the second type attack detection data or the IP packets having the destination IP address in the second type attack detection data, if the second type attack detection data is not provided to the director 6 before the each corresponding predetermined time (for two minutes and for two seconds) elapses, blocking of the entry into the LAN 1 by the IP packets having the source IP address of the second attack detection data or IP packets having the destination IP address of the second attack detection data is released. In this manner, the sensor 5 that completes processing detection of the attack of SYN FLOOD proceeds to processing detection of the third type attack (Teardrop). In this processing, the sensor 5 sequentially extracts IP packets that are split (hereinafter, simply "split packets") and that are included in the each IP packet group having the identical destination IP address that belongs to the LAN 1. In this case, in IP, a certain flag in the IP header is one or the data that is so-called fragment offset has larger value than zero for the split packets, whereby the split packets can be found. The sensor 5 checks for presence of packets in the IP packet group identical to the split packets that are acquired within the predetermined time (for example, in five minutes) from the time of acquiring the extracted each split packets and the fragment offset value and the IP identification number in the IP header are identical to those for the split packets (split packets identical to the extracted split packets). If such split packets present, the sensor 5 counts the number of the split packets including the previously extracted split packets. If the count is equal to or greater than the predetermined number (for example, 80), an attack of Teardrop is detected and the data indicative of the attack, the value data for the source IP address of the split packets and the value data

for the destination IP address (hereinafter, "third attack detection data") of the IP packets for which the attack is detected are provided to the director 6. Such processing is performed sequentially for all IP packet groups having the identical destination IP address that belongs to LAN 1. The director 6 that is provided with the third attack detection data from the sensor 5 controls the firewall 2 in the same manner as the case for detecting the SYN FLOOD. In other words, the director 6 rewrites the filter setting file of the firewall 2 to block the entry of the IP packets having the identical source IP address to the source IP address included in the third type attack detection data into the LAN 1 for predetermined time (for two minutes) from the present time. Simultaneously, the director 6 rewrites the filter setting file of the firewall 2 to block the entry of the IP packets that have the identical destination IP address to the destination IP address included in the third type attack detection data for predetermined time (for two minutes) from the present time, whereby the LAN 1 is protected from the attack of Treardrop and the host having the attacking target IP address can be resumed to the normal state without shutting down. In this manner, after the sensor 5 completes processing for detecting an attack of Treardrop, the sensor 5 performs processing for fourth type attack detection (LAND). In this processing, from the each IP packet group having the destination IP address that belongs to the LAN 1 in the IP packet groups having the identical destination IP address, the sensor 5 extracts IP packets having the source IP address identical to the value for the destination IP address in the IP packet group. Furthermore, the sensor 5 checks for presence of the IP packets that are acquired within the predetermined time (for example, in two minutes) from the time of acquiring the IP packets and that have the

identical source IP address to that for the IP packets in the IP packet group having the destination IP address identical to that for the extracted IP packets. If such IP packets present, the number of the IP packets including the previously extracted IP packets is counted. If the count is equal to or greater than the predetermined number (for example, 6), an attack of LAND is detected and the data indicative of the attack, the value data for the source IP address of the IP packets for which the attack is detected (hereinafter, "fourth attack detection data") are provided to the director 6. Such processing is performed sequentially for all IP packet groups having the identical destination IP address that belongs to LAN 1. The director 6 that is provided with the fourth attack detection data from the sensor 5 rewrites the filter setting file of the firewall 2 to block the entry into the LAN 1 by the IP packets that have the identical source IP address to the source IP address included in the fourth type attack detection data and that have the identical destination IP address to the source IP address for predetermined time (for example, for five minutes) from the present time. At this time, upon receiving the IP packets having the source IP address and the IP packets having the destination IP address from the internet 3, the firewall 2 discards the IP packets to block the entry thereof into the LAN 1, whereby the LAN 1 is protected from the attack of LAND. Similarly to the case for detecting port scanning, if the director 6 is again provided by the sensor 5 with the fourth type attack detection data identical to the fourth type attack detection data that is previously provided before the predetermined time (five minutes) elapses for eliminating the IP packets having the source IP address and the destination IP address identical to the source IP address in the fourth type attack detection data, the director 6

controls the firewall 2 to block the entry into the LAN 1 by the IP packets having the source IP address and the destination IP address of the fourth attack detection data for the predetermined time (for five minutes) from the moment that the director 6 is provided with the fourth attack detection data. Accordingly, unless attacking of LAND continues, the IP packets having the source IP address and the destination IP address associated with attacking cannot enter into the LAN 1. If the fourth attack detection data is not provided, the director 6 releases the blocking of the entry into the LAN 1 by the IP packets having the source IP address and the destination IP address identical to the source IP address of the fourth attack detection data.

[0009] In the present embodiment, the value data for the source IP address of the IP packets associated with the attack of LAND is made to be provided to the director 6 as the fourth attack detection data. Because the source IP address has the same value as that for the destination IP address of the IP packets associated with the attack of LAN, alternatively for the value data for the source IP address, the value for the destination IP address can be provided to the director 6. As mentioned above, after the sensor 5 completes processing for detecting the attack of LAND, the sensor 5 performs processing for fifth type attack detection (acquiring password). In this processing, for the IP groups having the identical destination IP address, the sensor 5 extracts IP packets that include the user name data and the password data for the host of the LAN 1 for the each IP packet group having the destination IP address that belongs to the LAN 1. The sensor 5 counts the number of the IP packets acquired within a predetermined continuous time (for example, within two minutes) having the identical user name data and different password data

from the extracted IP packets. When the counted number is equal to or greater than the predetermined number (for example, 20), the sensor 5 detects a fifth type attack for acquiring a password and sends the data indicative of the attack together with the value data for the source IP address and the value data for the destination IP address (hereinafter, "fifth type attack detection data") of the IP packets for which the attack is detected to the director 6. Such processing is performed sequentially for all IP packet groups having the identical destination IP address that belongs to LAN 1. The director 6 that is provided with the fifth attack detection data from the sensor 5 rewrites the filter setting file of the firewall 2 to block the entry into the LAN 1 by the IP packets that have the source IP address and the destination IP address identical to the source IP address and the destination IP address of the fifth type attack detection data for predetermined time (for example, for one hour) from the present time. At this time, upon receiving the IP packets having the source IP address or having the destination IP address from the internet 3, the firewall 2 discards the IP packets to block the entry thereof into the LAN 1, whereby the LAN 1 is protected from the fifth type attack aiming at acquiring the password. Similarly to the case for detecting port scanning, if the director 6 is again provided by the sensor 5 with the fifth type attack detection data identical to the fifth type attack detection data that is previously provided before predetermined time (one hour) elapses for eliminating the IP packets having the source IP address and the destination IP address identical to those in the fifth type attack detection data, the director 6 controls the firewall 2 to block the entry into the LAN 1 by the IP packets having the source IP address and the destination IP address of the fifth attack detection data for the

predetermined time (one hour) from the moment that the director 6 is provided with the fifth attack detection data. Accordingly, unless the fifth type attack continues, the IP packets having the source IP address and the destination IP address associated with the attacking cannot enter into the LAN 1. If the director 6 is not provided with the fifth type attack detection data again before the predetermined time (one hour) elapses, blocking of the entry into the LAN 1 by the IP packets having the source IP address and the destination IP address of the fifth type attack detection data is released. In this manner, after the sensor 5 completes processing for detecting the attack of LAND, the sensor 5 performs processing for sixth type attack detection (attacking through hole). In the processing, for the IP packet groups having the identical destination IP address, the sensor 5 retrieves IP packets having, for example, "lpr" command as the printer logical name with a data size being equal to or greater than 128 characters for the each IP packet group having the destination IP address that belongs to LAN 1. If such IP packets are retrieved, the sixth type attacking on the through hole of the host of LAN 1 is detected, and the data indicative of the attack, the value data for the source IP address and the value data for the destination IP address of the IP packets for which the attack is detected (hereinafter, "sixth attack detection data") are provided to the director 6. The director 6 that is provided with the sixth attack detection data from the sensor 5 rewrites the filter setting file of the firewall 2 to block the entry into the LAN 1 by the IP packets having the source IP address and the destination IP address identical to the source IP address and the destination IP address of the sixth type attack detection data for predetermined time (for example, for six hours) from the present time. At this time, upon receiving the IP

packets having the source IP address or the destination IP address from the internet 3, the firewall 2 discards the IP packets to block the entry thereof into the LAN 1, whereby the LAN 1 is protected from the sixth type attack on the through hole of the host of the LAN 1. Similarly to the case for detecting port scanning, if the director 6 is again provided with the sixth type attack detection data identical to the sixth type attack detection data that is previously provided from the sensor 5 before the predetermined time (six hours) elapses for eliminating the IP packets having the source IP address and the destination IP address identical to those in the sixth type attack detection data, the director 6 controls the firewall 2 to block the entry into the LAN 1 by the IP packets having the source IP address and the destination IP address of the sixth attack detection data for the predetermined time (six hours) from the moment that the director 6 is provided with the sixth attack detection data. Accordingly, unless the sixth type attack continues, the IP packets having the source IP address and the destination IP address associated with the attacking cannot enter into the LAN 1. If the director 6 is not provided with the sixth type attack detection data again before the predetermined time (six hours) elapses, blocking of the entry into the LAN 1 by the IP packets having the source IP address and the destination IP address of the sixth type attack detection data is released. As explained above, according to the system of the present embodiment, only introducing the sensor 5 and the director 6 enables real-time detection of various attacks on the LAN 1 by crackers and taking appropriate countermeasure promptly and automatically to protect the LAN 1 from the detected attack, thereby extensively reducing workload for a network administrator such as establishing the LAN 1 considering an attack by a cracker

or frequently referring a log file, leading to reduction of the management cost for the LAN 1. Furthermore, various attacks by the crackers can be detected in real time, so that in the state that no attack is detected, necessity for restricting communication between the LAN 1 and the external can be reduced, whereby the degree of freedom for communication by the LAN 1 in the normal state can be enhanced and the information resource on the internet 3 is effectively utilized. In the embodiment explained above, by providing the firewall 2 in the entrance for the LAN 1 and controlling the firewall 2 when detecting an attack by a cracker, the detected attack is automatically eliminated. Alternatively, when detecting the attack by the cracker, the processing can be simply performed such that the attack is notified to the network administrator, an expert security administrator, and the like. In this case, for example, the director 6 or the sensor 5 is connected to the host for the network administrator, the expert security administrator, or the like via a public line or an exclusive line. If detecting an attack, the information such as the first to sixth attack detection data are sent to the host for the network administrator, the expert security administrator, and the like from the director 6 or the sensor 5. If configured in this manner, the specific countermeasure for protecting the LAN 1 from the detected attack is taken directly by the network administrator or the like. In this case also, the network administrator or the like can take the countermeasure when notified. Moreover, the type of the attack is detected, so that the countermeasure against the attack can be taken relatively easily.

[Brief description of the drawings]

[Fig. 1] A diagram of a system configuration of a cracker

monitoring system according to an embodiment of the present invention.

[Description of the numerals]

1 LAN (network)

2 Firewall (packet filter)

3 Internet

4 Hub

5 Sensor (attack detecting unit)

6 Director (processing unit)

7 Ethernet card

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－57554
（P2001－57554A）
(43)公開日　平成13年２月27日(2001.2.27)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ 12/24		Ｈ０４Ｌ 11/08		５Ｋ０３０
12/26		11/00	３１０Ｃ	５Ｋ０３３
12/46		11/20	Ｂ	
12/28			１０２Ｚ	
12/66				

審査請求　未請求　請求項の数28　書面　（全 15 頁）　最終頁に続く

(21)出願番号　特願平11－265942

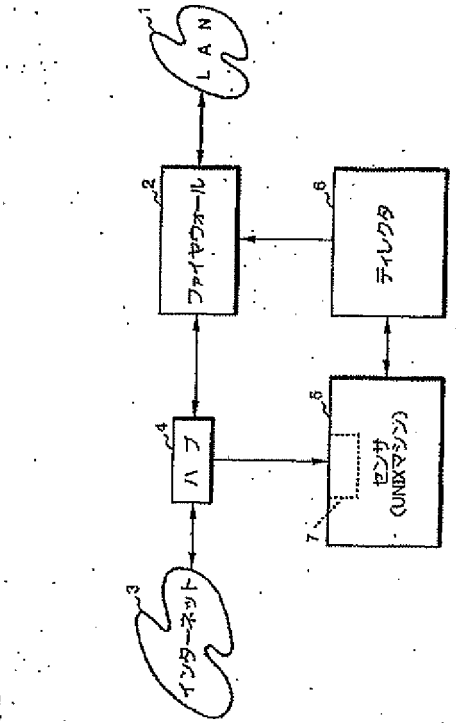
(22)出願日　平成11年８月17日(1999.8.17)

(71)出願人　398069654
馬場　芳美
千葉県八千代市村上2135－８
(72)発明者　馬場　芳美
千葉県八千代市村上2135－７　サンライフ91　202号

Ｆターム(参考)　5K030 GA15 HA08 HB28 HC14 JA10 MB18 MC08
5K033 AA08 BA08 CC02 DA06 DB20 EA06

(54)【発明の名称】　クラッカー監視システム

(57)【要約】
【課題】ネットワークに対するクラッカーからの攻撃を自動的に検知し、通信を必要以上に制限したり、熟練技術者による労力を必要とすることなく、簡易なシステム構成でクラッカーからの攻撃に対するネットワークの保護を図ることができるクラッカー監視システムを提供する。
【解決手段】ＬＡＮ１の入り口にそこを通るＩＰパケットを逐次取得するセンサ５を設ける。センサ５は、取得したＩＰパケットに基づき、ＬＡＮ１に対するクラッカーからの各種攻撃を検知する。センサ５が検知した攻撃に関する情報は、ファイヤウォール２を制御するディレクタ６に与えらる。ディレクタ６は与えられた情報に応じてファイヤウォール２の設定を制御し、検知された攻撃に係るＩＰパケットがＬＡＮ１に進入するのを阻止する。



(図１)

1

【特許請求の範囲】

【請求項１】ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）に基づく通信を行うネットワークの入り口において該入り口を通過するＩＰパケットを逐次取得し、取得したＩＰパケットを監視することにより該ネットワークに対するクラッカーからの攻撃を検知する攻撃検知手段と、該攻撃検知手段が前記攻撃を検知したとき、それに応じた所定の処理を行う処理手段とを備えたことを特徴とするクラッカー監視システム。

【請求項２】前記攻撃検知手段は、前記ネットワークの入り口を通過する全てのＩＰパケットを受信可能に構成されていることを特徴とする請求項１記載のクラッカー監視システム。

【請求項３】前記攻撃検知手段は、ＩＰパケットの受信のみが可能に構成されていることを特徴とする請求項２記載のクラッカー監視システム。

【請求項４】前記攻撃検知手段は、複数の種類の前記攻撃に対して、各種類の攻撃を検知するためのアルゴリズムを保持しており、取得したＩＰパケットから前記アルゴリズムに基づき各種類の攻撃を検知することを特徴とする請求項１～３のいずれか１項に記載のクラッカー監視システム。

【請求項５】前記攻撃検知手段は、所定時間内に取得した複数のＩＰパケットを少なくとも送信元ＩＰアドレス及び／又は宛先ＩＰアドレスにより分類して保持する手段を具備し、その分類したＩＰパケットから前記各種類の攻撃を検知することを特徴とする請求項４記載のクラッカー監視システム。

【請求項６】前記攻撃検知手段は、前記ネットワークにその外部から送信されてきた複数のＩＰパケットであって、少なくともその送信元ＩＰアドレスが互いに同一で且つ宛先ＩＰアドレス又は宛先ポート番号が互いに異なるものが所定時間内に所定数以上取得されたとき、第１の種類の前記攻撃がなされたことを検知することを特徴とする請求項１～５のいずれか１項に記載のクラッカー監視システム。

【請求項７】前記攻撃検知手段は、前記ネットワークにその外部から送信されてきたＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）に基づく複数のＳＹＮ用ＩＰパケットであって、少なくともその宛先ＩＰアドレスが互いに同一であるものが所定時間内に所定数以上取得され、且つ、その各ＳＹＮ用ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有すると共に前記ＴＣＰに基づくＡＣＫ用ＩＰパケットが前記所定時間内に取得されなかったとき、第２の種類の前記攻撃がなされたことを検知することを特徴とする請求項１～５のいずれか１項に記載のクラッカー監視システム。

【請求項８】前記攻撃検知手段は、前記ネットワークからその外部に送信されたＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）に基づく複数のＳＹＮ／ＡＣＫ用ＩＰパケットであって、少なくともその送信元ＩＰアドレスがそれぞれ互いに同一であるものが所定時間内に所定数以上取得され、且つ、前記ＴＣＰに基づくＡＣＫ用ＩＰパケットであって、前記各ＳＹＮ／ＡＣＫ用ＩＰパケットの送信元ＩＰアドレス及び宛先ＩＰアドレスとそれぞれ同一の宛先ＩＰアドレス及び送信元ＩＰアドレスを有するものが前記所定時間内に取得されなかったとき、第２の種類の前記攻撃がなされたことを検知することを特徴とする請求項１～５のいずれか１項に記載のクラッカー監視システム。

【請求項９】前記攻撃検知手段は、前記ネットワークにその外部から送信されてきた複数の分割されたＩＰパケットであって、同一の分割部分が所定時間内に所定数個以上取得されたとき、第３の種類の前記攻撃がなされていることを検知することを特徴とする請求項１～５のいずれか１項に記載のクラッカー監視システム。

【請求項１０】前記攻撃検知手段は、前記ネットワークにその外部から送信されてきた複数のＩＰパケットであって、その送信元ＩＰアドレスが宛先ＩＰアドレスと同一のアドレスとなっているものが所定時間内に所定数個以上取得されたとき、第４の種類の前記攻撃がなされていることを検知することを特徴とする請求項１～５のいずれか１項に記載のクラッカー監視システム。

【請求項１１】前記攻撃検知手段は、前記ネットワーク内の特定のホストを操作すべく該ネットワークにその外部から送信されてきた複数のＩＰパケットであって、前記特定のホストに係るユーザ名データが互いに同一で、且つパスワードが互いに異なるものが所定時間内に所定数以上取得したとき、第５の種類の前記攻撃がなされていることを検知することを特徴とする請求項１～５のいずれか１項に記載のクラッカー監視システム。

【請求項１２】前記攻撃検知手段は、バッファオーバフローと言われるセキュリティホールを攻撃する所定のパターンのデータを有するデータ列を有するＩＰパケットを取得したとき、第６の種類の前記攻撃がなされていることを検知することを特徴とする請求項１～５のいずれか１項に記載のクラッカー監視システム。

【請求項１３】前記処理手段が行う処理は、前記攻撃が検知された旨を表す報知出力を発生する処理であることを特徴とする請求項１～１２のいずれか１項に記載のクラッカー監視システム。

【請求項１４】前記処理手段が行う処理は、前記攻撃検知手段が検知した前記攻撃に係る特定の送信元ＩＰアドレス及び／又は宛先ＩＰアドレスを有するＩＰパケットの前記ネットワークへの進入を阻止する処理であることを特徴とする請求項１～１２の記載のクラッカー監視システム。

【請求項１５】前記処理手段が行う処理は、前記攻撃検知手段が前記第１の種類の攻撃を検知してから所定時

2

間、前記攻撃検知手段が検知した前記第１の種類の攻撃に係る前記送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求項６記載のクラッカー監視システム。

【請求項１６】前記処理手段が行う処理は、前記攻撃検知手段が前記第２の種類の攻撃を検知してから所定時間、前記各ＳＹＮ用ＩＰパケットと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求項７記載のクラッカー監視システム。

【請求項１７】前記処理手段が行う処理は、前記攻撃検知手段が前記第２の種類の攻撃を検知してから所定時間、前記各ＳＹＮ用ＩＰパケットと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理を含むことを特徴とする請求項１６記載のクラッカー監視システム。

【請求項１８】前記各ＳＹＮ用ＩＰパケットと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間は、前記各ＳＹＮ用ＩＰパケットと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定されていることを特徴とする請求項１７記載のクラッカー監視システム。

【請求項１９】前記処理手段が行う処理は、前記攻撃検知手段が前記第２の種類の攻撃を検知してから所定時間、前記各ＳＹＮ／ＡＣＫ用ＩＰパケットの送信元ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求項８記載のクラッカー監視システム。

【請求項２０】前記処理手段が行う処理は、前記攻撃検知手段が前記第２の種類の攻撃を検知してから所定時間、前記各ＳＹＮ／ＡＣＫ用ＩＰパケットの宛先ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理を含むことを特徴とする請求項１９記載のクラッカー監視システム。

【請求項２１】前記各ＳＹＮ／ＡＣＫ用ＩＰパケットの宛先ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間は、前記各ＳＹＮ／ＡＣＫ用ＩＰパケットの送信元ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定されていることを特徴とする請求項２０記載のクラッカー監視システム。

【請求項２２】前記処理手段が行う処理は、前記攻撃検知手段が前記第３の種類の攻撃を検知してから所定時間、前記分割されたＩＰパケットに係る宛先ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求項９記載のクラッカー監視システム。

【請求項２３】前記処理手段が行う処理は、前記攻撃検知手段が前記第３の種類の攻撃を検知してから所定時間、前記分割されたＩＰパケットに係る送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理を含むことを特徴とする請求項２２記載のクラッカー監視システム。

【請求項２４】前記分割されたＩＰパケットに係る送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間は、前記分割されたＩＰパケットに係る宛先ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定されていることを特徴とする請求項２３記載のクラッカー監視システム。

【請求項２５】前記処理手段が行う処理は、前記攻撃検知手段が前記第４の種類の攻撃を検知してから所定時間、該第４の種類の攻撃に係る前記ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求項１０記載のクラッカー監視システム。

【請求項２６】前記処理手段が行う処理は、前記攻撃検知手段が前記第５の種類の攻撃を検知してから所定時間、該第５の種類の攻撃に係る前記ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求項１１記載のクラッカー監視システム。

【請求項２７】前記処理手段が行う処理は、前記攻撃検知手段が前記第６の種類の攻撃を検知してから所定時間、該第６の種類の攻撃に係る前記ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求項１２記載のクラッカー監視システム。

【請求項２８】前記ネットワークの入り口には、該ネットワークに進入を阻止するＩＰパケットを選択的に設定可能なパケットフィルタが設けられ、前記処理手段は、前記処理を該パケットフィルタを制御することにより行うことを特徴とする請求項１４～２７のいずれか１項に記載のクラッカー監視システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

【０００２】本発明は、クラッカーによるネットワークへの攻撃を監視し、さらにはその攻撃からネットワークを保護するためのシステムに関する。

【従来の技術】

【０００３】近年、企業などの組織内に構築されたネットワーク（ＬＡＮ）は、その多くがインターネットに接続され、他のネットワーク等との間での各種情報のやりとり（通信）がインターネットを介して行われている。この通信では、一般に、所謂ＯＳＩ階層モデルにおけるネットワーク層に対応するプロトコルとしてＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）が用いられ、通信データはＩＰパケットの形態でやりとりされる。そして、上記ネットワーク層の上位のトランスポート層に対応するプロトコル（ＩＰの上位のプロトコル）として、ＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　ＣｏｎｔｒｏｌＰｒｏｔｏｃｏｌ）あるいはＵＤＰ（Ｕｓｅｒ　Ｄａｔａｇｒａｍ　Ｐｒｏｔｏｃｏｌ）を用いるのが通例である。この種のネットワークは、インターネット上のサーバや他のネットワークなどとの間で、多種多様な情報のやりとりを低コストで行うことができるという利点を有する反面、インターネットが極めて高度な公開性を有することから、所謂クラッカーからの攻撃を受ける危険性にさらされることとなる。このため、そのような攻撃からネットワークを保護することが要求される。このようなネットワークの保護を行うためのシステムとしては、従来、保護しようとするネットワークの入り口に、ファイヤウォール（詳しくはファイヤウォールの機能をもたせたコンピュータ）を設けたシステムが知られている。このファイヤウォールは、あらかじめネットワーク管理者などがネットワーク内への進入を阻止すべきものとして定めた種類の通信データ（ＩＰパケット）がネットワーク内に進入するのを阻止し、それ以外の許可された通信データのみを通過させるパケットフィルタとして機能するものである。この場合、ネットワーク内への進入を阻止する通信データの種類は、例えばＩＰパケットに含まれる送信元ＩＰアドレスや宛先ＩＰアドレス、宛先ポート番号などによって指定可能とされている。このようなファイヤウォールによれば、ネットワーク内の特定のＩＰアドレスを有するホスト（コンピュータ）、あるいはそのホストの特定のポート番号に対する外部からのアクセスを禁止したり、ネットワークの外部の特定のＩＰアドレス以外のＩＰアドレスからのネットワークへのアクセスを禁止したりすることができる。従って、ネットワークへの進入を禁止する通信データの種類をファイヤウォールに対して適切に設定しておけば、ネットワークへの攻撃の危険性を低減することが可能である。しかしながら、この種のファイヤウォールでは、その設定を適切に行うためには、通信技術やネットワーク技術、クラッカーによる攻撃手法など、ネットワークに関連した幅広い範囲の技術に対する高度の知識と理解が必要であると共に、個々のネットワークの構造や運用形態についても熟知している必要がある。つまり、ファイヤウォールにより阻止する通信データの種類は、それにより保護しようとするネットワークの各ホストがどのような情報を利用し、もしくは外部に提供し、また、ネットワーク内のどのような情報を保護すべきか、予想される攻撃としてどのようなものが想定されるか、ということなどを総合的に考慮して決定しなければならず、このためには、ネットワーク関連の高度な熟練技術者を要する。そして、特に保護しようとするネットワークの規模が比較的大きい場合や、該ネットワークで扱う情報が多岐にわたるような場合には、熟練技術者といえども、ファイヤウォールの適切な設定を行うことは困難である。さらに、ネットワークの構成を変更したような場合や、クラッカーからの攻撃を実際に受けたような場合、あるいは新たな手法の攻撃が出現したような場合には、多くの場合、ファイヤーウォールの設定内容を構築し直す必要があり、ファイヤウォールを含めたシステムの継続的な運営管理が必要となる。従って、ファイヤウォールの設定や、その管理運営には、熟練技術者による多大な労力やコストを要するものとなっていた。また、上記のような従来のファイヤウォールは、攻撃の可能性のある通信をすべて排除しようとするものであり、設定により禁止された種類の通信は、その通信がクラッカーからの攻撃によるものであるか否かにかかわらず一律的に排除される。つまり、ネットワークと外部との通信の自由度が必要以上に制限される。このため、ファイヤウォールを備えたネットワークでは、インターネット上の利用可能な情報提供サービスの制限を受け、インターネット上の多くの情報資源を有用に享受することができないという不都合を生じるものであった。

【発明が解決しようとする課題】

【０００４】本発明はかかる背景に鑑みてなされたものであり、ネットワークに対するクラッカーからの攻撃を自動的に検知し、通信を必要以上に制限したり、熟練技術者による労力を必要とすることなく、簡易なシステム構成でクラッカーからの攻撃に対するネットワークの保護を図ることができるクラッカー監視システムを提供することを目的とする。

【課題を解決するための手段】

【０００５】本発明のクラッカー監視システムは、かかる目的を達成するために、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）に基づく通信を行うネットワークの入り口において該入り口を通過するＩＰパケットを逐次取得し、取得したＩＰパケットを監視することにより該ネットワークに対するクラッカーからの攻撃を検知する攻撃検知手段と、該攻撃検知手段が前記攻撃を検知したとき、それに応じた所定の処理を行う処理手段とを備えたことを特徴とするものである。すなわち、本願発明者等がクラッカーによる各種攻撃の手法を検討したところ、多くの種類の攻撃は、そのそれぞれがＩＰパケット内のデータやＩＰパケットの通信形態に特徴がある。従って、前記ネットワークの入り口でそこを通過するＩＰパ

ケットを前記攻撃検知手段によって逐次取得し、その取得したＩＰパケットを監視することで、クラッカーによる前記ネットワークへの攻撃をリアルタイムで検知することができる。そして、このように攻撃を検知できれば、それに応じて前記処理手段により適当な処理（例えばネットワーク管理者などへの報知や、クラッカーによる通信を遮断する処理等）を行うことで、その攻撃からのネットワークの保護を図ることができる。この場合、クラッカーによる攻撃が十分に進行するまでには、一般に長い時間を要するため、攻撃が検知された時点、あるいは、それから若干遅れた時点でネットワークを保護するための処置を行っても、ネットワークの損害を十分に抑えることができる。このような本発明のシステムによれば、クラッカーによる攻撃をリアルタイムで検知できるので、その検知がなされたときに攻撃に対する対策処置を施せばよい。このため、ネットワーク管理者等は、所謂ログファイル（通信記録簿）等を頻繁に参照したりする必要性が低減されると共に、ネットワークの構築や再編等の際に、クラッカーによる攻撃を予測的に考慮するような労力が軽減される。また、攻撃が検知されない通常時は、ネットワークとその外部との通信を、攻撃の可能性を予測して制限する必要性がなく、その通信の自由度を高めることができる。従って、本発明によれば、ネットワークに対するクラッカーからの攻撃を自動的に検知し、通信を必要以上に制限したり、熟練技術者による労力を必要とすることなく、簡易なシステム構成でクラッカーからの攻撃に対するネットワークの保護を図ることができる。かかる本発明においては、前記攻撃検知手段は、前記ネットワークの入り口を通過する全てのＩＰパケットを受信可能に構成しておく。これにより、クラッカーによる多くの種類の攻撃を速やかに検知することが可能となる。さらに、本発明では、前記攻撃検知手段は、ＩＰパケットの受信のみが可能に構成しておく。これによれば、前記攻撃検知手段は、自己のＩＰアドレスやＭＡＣ（ＭｅｄｉａＡｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレス等、自己情報のデータをネットワークに送信することがないため、クラッカーなどによりその存在が認識されたり、攻撃の対象とされることがない。従って、攻撃検知手段の安全性を確保し、ひいては、本発明のシステムの信頼性を確保することができる。また、本発明では、前記攻撃検知手段は、複数の種類の前記攻撃に対して、各種類の攻撃を検知するためのアルゴリズムを保持しており、取得したＩＰパケットから前記アルゴリズムに基づき各種類の攻撃を検知する。これにより、クラッカーによる複数の種類の攻撃を検知することが可能となり、前記ネットワークの安全性を高めることができる。また、前記アルゴリズムを適宜更新することで、新しい種類の攻撃に対しても対応することが可能となる。この場合、前記攻撃検知手段は、所定時間内に取得した複数のＩＰパケットを少なくとも送信元ＩＰアドレス及び／又は宛先ＩＰアドレスにより分類して保持する手段を具備し、その分類したＩＰパケットから前記各種類の攻撃を検知する。すなわち、複数の種類の攻撃を検知するためには、ＩＰパケットの送信元ＩＰアドレスや宛先ＩＰアドレス（これらはＩＰパケットのＩＰヘッダに付与されている）が重要な鍵となることが多い。従って、所定時間内に取得したＩＰパケットを送信元ＩＰアドレス及び／又は宛先ＩＰアドレスにより分類して保持することで、それらのＩＰパケットから攻撃を検知しやすくなる。本発明では、より具体的には、前記攻撃検知手段は、次のように種々様々の攻撃を検知する。まず、クラッカーによる第１の種類の攻撃として、一般にポートスキャン（Ｐｏｒｔ　Ｓｃａｎ）と言われる種類の攻撃がある。この攻撃は、ネットワークに直接的な損害を及ぼすものではないが、その前段階の攻撃として用いられることが多い。この攻撃では、クラッカーは、自身の管理下にあるホストから、攻撃対象のネットワークに対して、パケット内の宛先ＩＰアドレスや宛先ポート番号を適宜変更しながらＩＰパケットを繰り返し送信する。そして、それらのＩＰパケットに対する応答を上記ホストを介して観測することで、攻撃対象のネットワークにおいて、ファイヤウォール等による制限を受けずに外部との通信に利用されているＩＰアドレスやポート番号を探索する。なお、ここで、前記ポート番号は、ＴＣＰあるいはＵＤＰ上で動作するアプリケーションソフトウェアのサービス種類（例えばｔｅｌｎｅｔ，ｆｔｐ，ｓｍｔｐ，ｔｆｔｐ等）を表すもので、ＩＰパケット内のＴＣＰヘッダあるいはＵＤＰヘッダに付与されるデータである。この種の攻撃では、上記のようなＩＰパケットの送信は、通常、専用的なツールソフトウェアを用いて行われ、攻撃対象のネットワークには、宛先ＩＰアドレスやポート番号が互いに異なり、且つ送信元ＩＰアドレスが同一であるようなＩＰパケットが比較的短時間内に多数、送信される。そこで、本発明では、前記攻撃検知手段は、前記ネットワークにその外部から送信されてきた複数のＩＰパケットであって、少なくともその送信元ＩＰアドレスが互いに同一で且つ宛先ＩＰアドレス又は宛先ポート番号が互いに異なるものが所定時間内に所定数以上取得されたとき、第１の種類の前記攻撃がなされたことを検知する。これにより、ポートスキャンと言われる第１の種類の攻撃を確実に検知することができる。次に、クラッカーによる第２の種類の攻撃として、一般にＳＹＮ　ＦＬＯＯＤと称される種類の攻撃がある。この攻撃は、ＴＣＰの特性を利用してネットワーク内の特定のホストをダウンさせるものである。すなわち、ＴＣＰでは二つのホスト間で通信を行う場合、まず、両ホスト間で論理的なコネクションの開設処理が行われる。このコネクション開設処理では、一方のホストから他方のホストに対してＳＹＮ用ＩＰパケットを送信する。ここで、該ＳＹＮ用ＩＰパケットは、それを詳しく言えば、

上記一方のホストのＩＰアドレスと他方のホストのＩＰアドレスとをそれぞれ送信元ＩＰアドレス、宛先ＩＰアドレスとしたＩＰパケットで、そのパケット内のＴＣＰヘッダのＳＹＮビット及びＡＣＫビットのうちのＳＹＮビットのみを「1」としたものである。そして、コネクション開設処理では、このＳＹＮ用ＩＰパケットを受けた他方のホストは、前記一方のホストに対してＳＹＮ／ＡＣＫ用ＩＰパケットを送信する。ここで、該ＳＹＮ／ＡＣＫ用ＩＰパケットは、詳しくは、上記他方のホストのＩＰアドレスと一方のホストのＩＰアドレスとをそれぞれ送信元ＩＰアドレス、宛先ＩＰアドレスとしたＩＰパケットで、そのパケット内のＴＣＰヘッダのＳＹＮビット及びＡＣＫビットを共に「1」としたものである。さらに、コネクション開設処理では、このＳＹＮ／ＡＣＫ用ＩＰパケットを受けた前記一方のホストは、前記他方のホストに対してＡＣＫ用ＩＰパケットを送信し、このＡＣＫ用ＩＰパケットを前記他方のホストが受けることで、両ホスト間の論理的なコネクションの開設がなされる。なお、上記ＡＣＫ用ＩＰパケットは、詳しくは、前記ＳＹＮ用ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットで、そのパケット内のＴＣＰヘッダのＳＹＮビット及びＡＣＫビットのうちのＡＣＫビットのみを「1」としたものである。前記ＳＹＮ　ＦＬＯＯＤは、このようなＴＣＰの特性を利用する攻撃であり、この攻撃では、クラッカーは、攻撃対象のネットワークの特定のホストに対して、比較的短い時間内に多数のＳＹＮ用ＩＰパケットを送信する。そして、それらの各ＳＹＮ用ＩＰパケットに対して上記特定ホストからＳＹＮ／ＡＣＫ用ＩＰパケットが送信されてきても、ＡＣＫ用ＩＰパケットをその特定ホストに送信しない。このような攻撃がなされたとき、上記特定ホストは、最初に送信されてきたＳＹＮ用ＩＰパケットに対するＳＹＮ／ＡＣＫ用ＩＰパケットを送信した後、所定時間（一般に２分）は、その時間内にＡＣＫ用パケットが送信されてこない限り、そのＡＣＫ用パケットの受信待ち状態となる。そして、この状態で新たなＳＹＮ用パケットが送信されてくる毎に、上記特定ホストは、新たなＳＹＮ用パケットに応じたコネクション開設処理を順番に完結すべくその新たなＳＹＮ用パケットの情報を通信処理用のバッファ領域に蓄積していく。ところが、バッファ領域の大きさには限界があり、該バッファ領域が満杯になり、このようになると、前記特定ホストは、ＴＣＰの通信処理やＴＣＰ上のサービス処理を行うことができなくなり、これにより、特定ホストがダウンすることとなる。この種の攻撃（ＳＹＮ　ＦＬＯＯＤ）では、前述のように、比較的短い時間内に、比較的多くのＳＹＮ用ＩＰパケットが攻撃対象のネットワーク内の特定のホスト（特定のＩＰアドレスを有するホスト）に対して送信されてくる。また、これに応じて、当該特定のホストからネットワークの外部に向かって、比較的短い時間内に、多くのＳＹＮ／ＡＣＫ用ＩＰパケットが送信される。さらに、それらのＳＹＮ用ＩＰパケットあるいはＳＹＮ／ＡＣＫ用ＩＰパケットに対応して最終的に前記特定ホストに送信されてくるべきＡＣＫ用パケットがその特定ホストに送信されてこない。そこで、本発明では、前記攻撃検知手段は、前記ネットワークにその外部から送信されてきたＴＣＰに基づく複数のＳＹＮ用ＩＰパケットであって、少なくともその宛先ＩＰアドレスが互いに同一であるものが所定時間内に所定数以上取得され、且つ、その各ＳＹＮ用ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有すると共に前記ＴＣＰに基づくＡＣＫ用ＩＰパケットが前記所定時間内に取得されなかったとき、第２の種類の前記攻撃がなされたことを検知する。あるいは、前記攻撃検知手段は、前記ネットワークからその外部に送信されたＴＣＰに基づく複数のＳＹＮ／ＡＣＫ用ＩＰパケットであって、少なくともその送信元ＩＰアドレスがそれぞれ互いに同一であるものが所定時間内に所定数以上取得され、且つ、前記ＴＣＰに基づくＡＣＫ用ＩＰパケットであって、前記各ＳＹＮ／ＡＣＫ用ＩＰパケットの送信元ＩＰアドレス及び宛先ＩＰアドレスとそれぞれ同一の宛先ＩＰアドレス及び送信元ＩＰアドレスを有するものが前記所定時間内に取得されなかったとき、第２の種類の前記攻撃がなされたことを検知する。これにより、ＳＹＮ　ＦＬＯＯＤといわれる第２の種類の攻撃を確実に検知することができる。次に、クラッカによる第３の種類の攻撃として、一般にＴｅａｒｄｒｏｐと称される種類の攻撃がある。この攻撃は、ＩＰパケットの分断（所謂ＩＰフラグメント）に係る処理の特性を利用してネットワーク内の特定のホストをダウンさせるものである。すなわち、ＩＰパケットは、インターネット上をルータを介して転送される過程で、各ルータのデータ処理容量の関係上、分断されることがある。また、各ルータにおいてＩＰパケットが転送される際にエラーが生じることもあり、このような場合には、ルータは、ＩＰパケットの再送信を行う。このため、ＩＰパケットの宛先ＩＰアドレスのホストでは、分断された一部の同じＩＰパケットが、複数受信されるということもある。このようなことから、ＩＰに基づく通信では、最終的にＩＰパケットを受け取るホスト（宛先ＩＰアドレスのホスト）は、受け取ったＩＰパケットが分断されたものであるとき、残りの全ての分断部分のＩＰパケットを受信するまで、各分割部分のＩＰパケットを蓄積保持し、全ての分断部分のＩＰパケットを受信してから、それらを整理して元のＩＰパケットのデータを復元する処理を行う。前記Ｔｅａｒｄｒｏｐは、このようなＩＰパケットの分断に係る処理の特性を利用する攻撃であり、この攻撃では、クラッカーは、比較的短い時間内に、多数の同じ分断部分のＩＰパケットを攻撃対象のネットワークの特定のホストに送信した上で、残りの分断部分のＩＰパケットをその特

定ホストに送信する。このような攻撃がなされたとき、上記特定ホストは、最終的に残りの分轄部分のＩＰパケットを受信したときに、そのＩＰパケットと、先に送信されてきた多量の分割部分のＩＰパケットとから元のＩＰパケットのデータを復元しようとする処理を行うため、その処理に長時間を要するものとなる。このため、該特定ホストは、事実上、ダウンしてしまうこととなる。この種の攻撃（Ｔｅａｒｄｒｏｐ）では、前述の如く、比較的短い時間内に、多数の同じ分轄部分のＩＰパケットがネットワーク内の特定のホストに送信されてくる。そこで、本発明では、前記攻撃検知手段は、前記ネットワークにその外部から送信されてきた複数の分割されたＩＰパケットであって、同一の分割部分が所定時間内に所定数個以上取得されたとき、第３の種類の前記攻撃がなされていることを検知する。これにより、Ｔｅａｒｄｒｏｐといわれる第３の種類の攻撃を確実に検知することができる。次に、クラッカーによる第４の種類の攻撃として、一般にＬａｎｄと称される種類の攻撃がある。この攻撃は、送信元ＩＰアドレス及び宛先ＩＰアドレスが同一であるような、正規にはあり得ないＩＰパケットを、攻撃対象のネットワークの特定のホストに送信する攻撃である。このようなＩＰパケットを送信された特定ホストは、そのＩＰパケットの処理に手間取ることが多く、ダウンしてしまうことがしばしばある。この種の攻撃では、上記の如く、送信元ＩＰアドレス及び宛先ＩＰアドレスが同一であるＩＰパケットが、ネットワーク内の特定のホストに送信され、しかも、一般には、そのようなＩＰパケットが比較的短い時間内に、複数、上記特定ホストに送信される。そこで、本発明では、前記攻撃検知手段は、前記ネットワークにその外部から送信されてきた複数のＩＰパケットであって、その送信元ＩＰアドレスが宛先ＩＰアドレスと同一のアドレスとなっているものが所定時間内に所定数個以上取得されたとき、第４の種類の前記攻撃がなされていることを検知する。これにより、Ｌａｎｄとわれる第４の種類の攻撃を確実に検知することができる。次に、クラッカーによる第５の種類の攻撃として、ネットワーク内の特定のホストのユーザのパスワードを獲得する攻撃がある。この攻撃では、クラッカーは、攻撃対象のネットワーク内の特定のホストのユーザ名を使って、ｔｅｌｎｅｔ等により上記特定ホストにログインし、さらに所定の辞書ファイルなどから選択した多数のパスワードを使って、その特定ホストの操作を試みる。そして、このとき、その特定ホストの操作ができるか否かにより、パスワードが判明することとなる。この種の攻撃では、同一のユーザ名データを含み、しかも互いに異なるパスワードを有する多数のＩＰパケットが、攻撃対象のネットワークの特定ホストに送信される。そこで、本発明では、前記攻撃検知手段は、前記ネットワーク内の特定のホストを操作すべく該ネットワークにその外部から送信されてきた複数のＩＰパケットであって、前記特定のホストに係るユーザ名データが互いに同一で、且つパスワードが互いに異なるものが所定時間内に所定数以上取得したとき、第５の種類の前記攻撃がなされていることを検知する。これにより、上記のようにパスワードを獲得する攻撃を確実に検知することができる。次に、クラッカーによる第６の種類の攻撃として、ネットワーク内の特定のホストに、ネットワーク管理者など、ごく限られた者が、専用のパスワードを入力した状態でしか実行させることができないような処理（所謂、ルートコマンド）を行わせる攻撃がある。この攻撃は、攻撃対象のホストが搭載しているＯＳ（Ｏｐｅｒａｔｉｏｎ　Ｓｙｓｔｅｍ）のセキュリティホールといわれるバグを利用するものである。すなわち、例えばＵＮＩＸマシン（ホスト）は、バッファオーバフローといわれるセキュリティホールを有しており、このセキュリティホールは、例えばプリンタの論理名を表す「ｌｐｒ」というコマンドを含む比較的大きなデータ（１２８文字以上のデータ）が一度に送られてきたとき、バッファがオーバフローし、そのオーバフローしたデータ内に、ルートコマンドがあると、ネットワーク管理者などのパスワードが入力されていなくても、そのルートコマンドを実行してしまうというものである。前記第６の種類の攻撃は、このようなバッファオーバフローといわれるセキュリティホールを攻撃するもので、前述の「ｌｐｒ」というコマンドを含む所定サイズ以上のデータ列というような、所定のパターンのデータを含むデータ列を有するＩＰパケットがネットワークの特定のホストに送信される。そこで、本発明では、前記攻撃検知手段は、バッファオーバフローと言われるセキュリティホールを攻撃する所定のパターンのデータを有するデータ列を有するＩＰパケットを取得したとき、第６の種類の前記攻撃がなされていることを検知する。これにより、上記のような第６の種類の攻撃を検知することができる。前述のようにクラッカーによる攻撃を検知する攻撃検知手段を備えた本発明では、前記処理手段が行う処理は、例えば前記攻撃が検知された旨を表す報知出力を発生する処理である。この報知出力の発生により、ネットワーク管理者やあるいは外部の専門技術者等が、検知された攻撃を排除するための処置を施すことが可能となる。

【０００６】あるいは、前記処理手段が行う処理は、前記攻撃検知手段が検知した前記攻撃に係る特定の送信元ＩＰアドレス及び／又は宛先ＩＰアドレスを有するＩＰパケットの前記ネットワークへの進入を阻止する処理である。これにより、クラッカーによるネットワークへの通信、あるいは、攻撃対象とされたホストへの通信が自動的に遮断され、攻撃の検知に応じたネットワークの保護をリアルタイムで図ることができる。より具体的には、ポートスキャンと言われる前記第１の種類の攻撃を検知したときには、前記処理手段が行う処理は、前記攻

撃検知手段が前記第１の種類の攻撃を検知してから所定時間、前記攻撃検知手段が検知した前記第１の種類の攻撃に係る前記送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理である。すなわち、前記送信元ＩＰアドレスが、クラッカーがポートスキャンの攻撃に使用しているホストのＩＰアドレスであるので、このＩＰアドレスを送信元ＩＰアドレスとしてネットワークに送信されてくるＩＰパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、クラッカーは、攻撃が検知されてから所定時間は、上記送信元ＩＰアドレスのホストからネットワークへの通信を行うことができなくなり、ネットワークに関する情報を取得することができなくなる。なお、このとき、ポートスキャンの攻撃が継続的に行われる限り、逐次、それが検知されるので、事実上、その攻撃が継続している間は、事実上、クラッカーは、ネットワークへの通信を行うことができなくなる。また、ＳＹＮ　ＦＬＯＯＤといわれる前記第２の種類の攻撃については、この攻撃を前述のようにＳＹＮ用ＩＰパケットに基づいて検知した場合には、前記処理手段が行う処理は、前記攻撃検知手段が前記第２の種類の攻撃を検知してから所定時間、前記各ＳＹＮ用ＩＰパケットと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理である。すなわち、前記各ＳＹＮ用ＩＰパケットの宛先ＩＰアドレスがＳＹＮ　ＦＬＯＯＤの攻撃の対象とされているホストのＩＰアドレスであるので、そのホストのＩＰアドレスを宛先ＩＰアドレスとするＩＰパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。また、ＳＹＮ　ＦＬＯＯＤの攻撃をＳＹＮ／ＡＣＫ用ＩＰパケットに基づいて検知した場合には、前記処理手段が行う処理は、前記攻撃検知手段が前記第２の種類の攻撃を検知してから所定時間、前記各ＳＹＮ／ＡＣＫ用ＩＰパケットの送信元ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理である。すなわち、前記各ＳＹＮ／ＡＣＫ用ＩＰパケットは、ＳＹＮ　ＦＬＯＯＤの攻撃を行おうとしているクラッカーの管理下にあるホストからネットワークに送信されてＳＹＮ用パケットに対して、ネットワーク内のホストがクラッカー側に応答するパケットであるので、前記各ＳＹＮ／ＡＣＫ用ＩＰパケットの送信元ＩＰパケットの送信元ＩＰアドレスが、ＳＹＮ　ＦＬＯＯＤの攻撃の対象とされているホストのＩＰアドレスである。従って、そのネットワーク内のホストのＩＰアドレスを宛先ＩＰアドレスとして、ネットワークに送信されたＩＰパケットを該ネットワークに対して遮断する。上記のように、ＳＹＮ　ＦＬＯＯＤの攻撃にかかるＩＰパケットがネットワークに進入するのを阻止することで、その攻撃の対象とされたネットワーク内のホストには、所定時間は、ＳＹＮ用ＩＰパケット等のＩＰパケットが送信されてこなくなる。この場合、攻撃対象とされたホストでは、先に送信されてきたＳＹＮ用ＩＰパケットに対してある程度の時間内（通常２分）にコネクション開設を正常に完結することができないと、自動的にコネクション開設の処理を中止する。従って、上記のようにＩＰパケットが所定時間、送信されてこなくなることで、その所定時間内に正常状態に復帰することができる。さらに、本発明では、ＳＹＮ　ＦＬＯＯＤの検知に応じて、前記処理手段が行う処理は、前記攻撃検知手段が前記第２の種類の攻撃を検知してから所定時間、前記各ＳＹＮ用ＩＰパケットと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理を含む。あるいは、前記攻撃検知手段が前記第２の種類の攻撃を検知してから所定時間、前記各ＳＹＮ／ＡＣＫ用ＩＰパケットの宛先ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理を含む。すなわち、ＳＹＮ　ＦＬＯＯＤでは、クラッカーがＳＹＮ用ＩＰパケットを送信するに際して、送信元ＩＰアドレスを偽ったり、送信元ＩＰアドレスを適宜変更したりすることもあるが、一般には、前記各ＳＹＮ用ＩＰパケットの送信元ＩＰアドレス、あるいはそれに対応したＳＹＮ／ＡＣＫ用ＩＰパケットの宛先ＩＰアドレスは、クラッカーの管理下にあるホストのＩＰアドレスである可能性が高い。従って、このようなＩＰアドレスを送信元ＩＰアドレスとして有するＩＰパケットは、攻撃が検知されてから所定時間はネットワークに対して遮断する。これにより、クラッカーの攻撃に対するネットワークの保護をより高めることができる。この場合さらに、前記各ＳＹＮ用ＩＰパケットと同一の送信元ＩＰアドレス、あるいは、前記各ＳＹＮ／ＡＣＫ用ＩＰパケットの宛先ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間は、前記ＳＹＮ用ＩＰパケットと同一の宛先ＩＰアドレス、あるいは、前記各ＳＹＮ／ＡＣＫ用ＩＰパケットの送信元ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定する。すなわち、ＳＹＮ　ＦＬＯＯＤの攻撃対象のホストへの通信を遮断する時間（上記の後者側の所定時間）は、該ホストがその攻撃に対して正常に復帰し得る程度の時間で十分である。これに対して、クラッカーの管理下にある可能性の高いホストからネットワークへの通信を遮断する時間（上記の前者側の所定時間）は、ネットワークの保護の観点から、比較的長いものとすることが好ましいと考えられる。従って、上記の前者側の所定時間を、後者側の所定時間よりも長く設定する。これにより、ネットワーク内のホストの外部との通信の自由度をできるだけ確保しつつ、ＳＹＮ　ＦＬＯＯＤに対するネットワークの保護も十分に図ることができ

る。また、Ｔｅａｒｄｒｏｐといわれる前記第３の種類の攻撃を検知した場合にあっては、前記処理手段が行う処理は、前記攻撃検知手段が前記第３の種類の攻撃を検知してから所定時間、前記分割されたＩＰパケットに係る宛先ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理である。すなわち、前記分轄されたＩＰパケットに係る宛先ＩＰアドレスが、Ｔｅａｒｄｒｏｐの攻撃の対象とされているホストのＩＰアドレスであるので、そのホストのＩＰアドレスを宛先ＩＰアドレスとするＩＰパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、Ｔｅａｒｄｒｏｐの攻撃の対象とされたネットワーク内のホストには、所定時間は、分轄されたＩＰパケット等のＩＰパケットが送信されてこなくなる。この場合、攻撃対象とされたホストでは、先に送信されてきた分轄部分のＩＰパケットに対応する残りのＩＰパケットが、ある程度の時間内（通常１分）に受信されないと、そのＩＰパケットに関する通信処理を自動的に中止する。従って、上記のようにＩＰパケットが所定時間、送信されてこなくなることで、その所定時間内に正常状態に復帰することができる。さらに、本発明では、Ｔｅａｒｄｒｏｐの検知に応じて、前記処理手段が行う処理は、前記攻撃検知手段が前記第３の種類の攻撃を検知してから所定時間、前記分割されたＩＰパケットに係る送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理を含む。すなわち、前述したＳＹＮ　ＦＬＯＯＤの場合と同様に、前記分轄されたＩＰパケットに係る送信元ＩＰアドレスは、クラッカーの管理下にあるホストのＩＰアドレスである可能性が高い。従って、このようなＩＰアドレスを送信元ＩＰアドレスとして有するＩＰパケットは、攻撃が検知されてから所定時間はネットワークに対して遮断する。これにより、クラッカーの攻撃に対するネットワークの保護をより高めることができる。この場合さらに、前記分割されたＩＰパケットに係る送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間は、前記分割されたＩＰパケットに係る宛先ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定する。すなわち、ＳＹＮ　ＦＬＯＯＤの場合と同様、Ｔｅａｅｄｒｏｐの攻撃対象のホストへの通信を遮断する時間（上記の後者側の所定時間）は、該ホストがその攻撃に対して正常に復帰し得る程度の時間で十分であるのに対して、クラッカーの管理下にある可能性の高いホストからネットワークへの通信を遮断する時間（上記の前者側の所定時間）は、ネットワークの保護の観点から、比較的長いものとすることが好ましいと考えられる。従って、上記の前者側の所定時間を、後者側の所定時間よりも長く設定する。これにより、ネットワーク内のホストの外部との通信の自由度をできるだけ確保しつつ、Ｔｅａｒｄｒｏｐに対するネットワークの保護も十分に図ることができる。

【０００７】また、ＬＡＮＤといわれる前記第４の種類の攻撃を検知した場合にあっては、前記処理手段が行う処理は、前記攻撃検知手段が前記第４の種類の攻撃を検知してから所定時間、該第４の種類の攻撃に係る前記ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理である。すなわち、ＬＡＮＤという攻撃では、送信元ＩＰアドレスと宛先ＩＰアドレスとが同一であるＩＰパケットが送信されてくるので、そのＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、ＬＡＮＤという攻撃からネットワークを保護することができる。また、ネットワーク内のホストのユーザのパスワードを獲得する前記第５の種類の攻撃を検知する場合にあっては、前記処理手段が行う処理は、前記攻撃検知手段が前記第５の種類の攻撃を検知してから所定時間、該第５の種類の攻撃に係る前記ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理である。すなわち、第５の種類の攻撃に係るＩＰパケットの宛先ＩＰアドレスは、攻撃対象とされたホストのＩＰアドレスであり、また、該ＩＰパケットの送信元ＩＰアドレスは、クラッカーの管理下にあるホストのＩＰアドレスである。従って、第５の種類の攻撃に係るＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、クラッカーは、種々のパスワードを有するＩＰパケットをネットワークの特定のホストに送信しても、その各パスワードで当該特定ホストを操作することができるのかどうかが判らなくなるので、上記第５の種類の攻撃からネットワークを保護することができる。また、セキュリティホールを利用した前記第６の種類の攻撃を検知する場合にあっては、前記処理手段が行う処理は、前記攻撃検知手段が前記第６の種類の攻撃を検知してから所定時間、該第６の種類の攻撃に係る前記ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理である。すなわち、第６の種類の攻撃に係るＩＰパケットの宛先ＩＰアドレスは、攻撃対象とされたホストのＩＰアドレスであり、また、該ＩＰパケットの送信元ＩＰアドレスは、クラッカーの管理下にあるホストのＩＰアドレスである。従って、第６の種類の攻撃に係るＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットを、攻撃が検知されて

から所定時間、ネットワークに対して遮断する。これにより、クラッカーは、ネットワーク内の特定のホストセキュリティホールを攻撃するＩＰパケットをネットワークの特定のホストに送信しても、該ＩＰパケットは、当該特定ホストに与えられなくなるので、当該特定ホストにルートコマンドを実行させることができなくなり、前記第６の種類の攻撃からネットワークを保護することができる。以上説明したように各種の攻撃に係るＩＰパケットのネットワークへの進入を、攻撃の検知に応じて自動的に行う本発明では、前記ネットワークの入り口に、該ネットワークに進入を阻止するＩＰパケットを選択的に設定可能なパケットフィルタを設けておき、前記処理手段は、前記処理を該パケットフィルタを制御することにより行う。これによれば、前記パケットフィルタとして、例えばファイヤウォールを用いることで、既存のシステムを流用しつつ本発明のシステムを構築することが可能となる。なお、ファイヤウォールよりもＩＰパケットの取捨・選択の機能は劣るが、一般にルータもパケットフィルタとしての機能を有しており、従って、前記パケットフィルタとしてルータを用いることも可能である。

【発明の実施の形態】

【０００８】本発明の一実施形態を図１を参照して説明する。図１は本実施形態のシステム構成図である。図１において、１はネットワークとしてのＬＡＮである。このＬＡＮ１は、例えばイーサネット（Ｅｔｈｅｒｎｅｔ）を用いて構築されたものであり、図示を省略する複数のホスト（コンピュータ）がイーサネット・ケーブルやハブ等を介して接続されている。各ホストには、それをイーサネット・ケーブルに接続するイーサネット・カードや、ＴＣＰ／ＩＰの処理を行うためのソフトウェア、ＴＣＰ／ＩＰ上で機能する各種アプリケーションソフトウェア（例えば、ｔｅｌｎｅｔ、ｆｔｐ、ｓｍｔｐ等）が実装され、ＩＰに基づく通信を可能としている。なお、ＬＡＮ１は、イーサネット上で構築されたものに限らず、トークンリング等、他の形態で構築されたものであってもよい。本実施形態のシステムでは、ＬＡＮ１の入り口に、パケットフィルタとしてのファイヤウォールの機能をもたせたコンピュータ２（以下、このコンピュータ２を単にファイヤウォール２と称する）が設けられており、ＬＡＮ１はファイヤウォール２を介してインターネット３に接続されている。ファイヤウォール２は、どのような種類のＩＰパケットのＬＡＮ１への進入を禁止するかを規定するデータが書き込まれるファイル（以下、フィルタ設定ファイルという）を有しており、このフィルタ設定ファイルで、ＬＡＮ１への進入が禁止された種類のＩＰパケットがインターネット３側から送信されてきたときに、そのＩＰパケットを廃棄してＬＡＮ１への進入を阻止する。そして、フィルタ設定ファイルで、ＬＡＮ１への進入が禁止されていないＩＰパケットが送信されてきたときには、それをＬＡＮ１に転送する。ファイヤウォール２とインターネット３との間には、ハブ４が介装され、このハブ４に攻撃検知手段の機能をもたせたセンサ５が接続されている。また、このセンサ５には、前記ファイヤウォール２を制御する処理手段の機能を有するディレクタ６が接続されている。これらのセンサ５及びディレクタ６はそれぞれコンピュータにより構成されたものである。前記センサ５は例えばＵＮＩＸマシンにより構成され、イーサネットカード７を介して前記ハブ４に接続されている。この場合、センサ５には、ＴＣＰ　ＤＵＭＰといわれるソフトウェアが実装されており、このＴＣＰ　ＤＵＭＰによって、ハブ４を通る全てのＩＰパケットをイーサネットカード７を介して取得する（ヒアリングする）ことができるようになっている。そして、センサ５は、取得した各ＩＰパケットをその取得時点の時刻データと共に図示しないハードディスクに記憶保持するようにしている。なお、ハードディスクに記憶保持したＩＰパケットの総量が所定の許容量に達したときには、センサ５は、最も古いＩＰパケットを消去し、新たに取得されたＩＰパケットをハードディスクに記憶保持する。また、センサ５は、ＩＰアドレスを持たず、ＡＲＰ（Ａｄｒｅｓｓ　ＲｅｓｏｌｕｔｉｏｎＰｒｏｔｏｃｏｌ）や、ＲＡＲＰ（Ｒｅｖｅｒｓｅ　ＡｄｒｅｓｓＲｅｓｏｌｕｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）のパケット等、応答を促すパケットが送信されてきても、それに対する応答をしないようにソフトウェア的に設定されており、ＩＰパケットの受信（取り込み）のみを行うことできるものとされている。さらに、センサ５には、前述した第１～第６の種類の攻撃を検知するためのソフトウェア（以下、攻撃検知アルゴリズム）が実装されている。なお、この攻撃検知アルゴリズムは、ディレクタ６に実装しておき、該ディレクタ６とのデータ授受を行いつつ該攻撃検知アルゴリズムの処理をセンサ５に行わせるようにしてもよい。前記ディレクタ６には、前記ファイヤウォール２を制御するソフトウェア（以下、フィルタ制御アルゴリズムという）が実装されている。この場合、フィルタ制御アルゴリズムは、センサ５により検知される攻撃に応じて、前記フィルタ設定ファイルのデータを適宜書き換えることで、前記ファイヤウォール２を制御するものである。次に、かかる本実施形態の作動を説明する。前記センサ５は、取得されるＩＰパケットを前述の如くハードディスクに記憶保持しつつ、所定のサイクルタイム毎に次のような処理を行う。すなわち、センサ５は、ハードディスクから所定の時間間隔分の複数のＩＰパケットを、送信元ＩＰアドレス及び宛先ＩＰアドレスの値別に分類（ソート）した上で、図示しないメモリに取り込んで保持する。つまり、所定の時間間隔分の複数のＩＰパケットのうち、同一の送信元ＩＰアドレスを有するものをひとまとめにすると共に、同一の宛先ＩＰアドレスを有するものをひとまとめ

にして、メモリに取り込む（以下の説明では、このようにひとまとめにされたＩＰパケットの組をＩＰパケット群という）。そして、このメモリに取り込んだ複数のＩＰパケットに対して、後述する攻撃検知の処理を行った上で、それらのＩＰパケットをメモリから消去する。この場合、各サイクルタイムにおいて、メモリに取り込むＩＰパケットは、前回のサイクルタイムでメモリに取り込んだＩＰパケットのうちの最も古いＩＰパケットの取得時刻から所定時間を経過した時刻以後に取得されたものである。各サイクルタイムにおけるセンサ５による攻撃検知の処理は、攻撃検知アルゴリズムに従って次のように行われる。センサ５は、まず、前記第１～第６の種類の攻撃のうち、例えば、第１の種類の攻撃、すなわちポートスキャンを検知する処理を行う。この処理では、センサ５は、メモリに前述のように取り込んだＩＰパケットのうち、送信元ＩＰアドレスが同一で、且つ該送信元ＩＰアドレスがＬＡＮ１の外部のものである各ＩＰパケット群に対し、その各ＩＰパケット群に含まれるＩＰパケットが有する全ての宛先ＩＰアドレスの値（これはＬＡＮ１に属するＩＰアドレスの値である）を抽出する。そして、上記の各ＩＰパケット群で抽出した宛先ＩＰアドレスの各値に対し、そのＩＰパケット群（同一の送信元ＩＰアドレスのＩＰパケット群）から、該宛先ＩＰアドレスの値と同一の宛先ＩＰアドレスを有し、且つＴＣＰヘッダあるいはＵＤＰヘッダ内の宛先ポート番号が互いに異なり、且つ、連続した所定時間内（例えば３０秒内）に取得されたＩＰパケットの個数をカウントする。このとき、このカウント数が所定数（例えば２０個）に達した場合には、センサ５は、ポートスキャンの攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知されたＩＰパケット群の送信元ＩＰアドレスの値データとを（以下、これらのデータを第１種攻撃検知データという）前記ディレクタ６に与える。このような処理が送信元ＩＰアドレスが同一で、且つ該送信元ＩＰアドレスがＬＡＮ１に属さない全てのＩＰパケット群に対し順次行われる。なお、本実施形態におけるポートスキャンの検知では、ポート番号が互いに異なるＩＰパケットの個数をカウントするようにしたが、次のような処理によりポートスキャンを検知するようにしてもよい。すなわち、送信元ＩＰアドレスが同一で、且つ、該送信元ＩＰアドレスがＬＡＮ１外部のものである各ＩＰパケット群に対し、その各ＩＰパケット群に含まれるＩＰパケットが有する全ての宛先ポート番号の値を抽出し、その抽出した宛先ポート番号の各値に対し、該宛先ポート番号を抽出したＩＰパケット群から、該宛先ポート番号の値と同一の宛先ポート番号を有し、且つ宛先ＩＰアドレスが互いに異なり、且つ、連続した所定時間内に取得されたＩＰパケットの個数をカウントする。そして、そのカウント数が所定数に達した場合にポートスキャンが行われていることを検知する。一方、センサ５から前述のような第１種攻撃検知データを与えられた前記ディレクタ６は、該第１種攻撃検知データに含まれる送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば５分間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール２は、上記送信元ＩＰアドレスを有するＩＰパケットがインターネット３から送信されてくると、そのＩＰパケットを廃棄し、ＬＡＮ１への進入を阻止する。これにより、ポートスキャンの攻撃からＬＡＮ１が保護される。なお、ディレクタ６は、上記所定時間（５分間）が経過するまでの間に、先に与えられた第１種攻撃検知データと同一の第１種攻撃検知データがセンサ５から再度与えられれば、その時点から上記所定時間（５分間）、該第１種攻撃検知データの送信元ＩＰアドレスからのＩＰパケットのＬＡＮ１への進入を阻止するようにファイヤウォール２を制御する。従って、ポートスキャンの攻撃が続いている限り、その送信元ＩＰアドレスからのＩＰパケットは、ＬＡＮ１に進入することはできない。そして、ディレクタ６は、上記所定時間（５分間）が経過するまでに、前記第１種攻撃検知データが与えられなかった場合には、その第１種攻撃検知データの送信元ＩＰアドレスからのＩＰパケットのＬＡＮ１への進入の阻止を解除する。前述のようにポートスキャンの攻撃の検知処理を行ったセンサ５は、次に、第２の種類の攻撃（ＳＹＮ　ＦＬＯＯＤ）の検知処理を行う。この処理では、センサ５は、宛先ＩＰアドレスが同一であるＩＰパケット群のうち、ＬＡＮ１に属する宛先ＩＰアドレスの各ＩＰパケット群に対し、該ＩＰパケット群に含まれるＳＹＮ用ＩＰパケットをその取得時刻順に順次抽出する。そして、抽出した各ＳＹＮ用ＩＰパケットの取得時刻から所定時間（例えば２秒間）内に取得されたＳＹＮ用ＩＰパケットが、同じ宛先ＩＰアドレスのＩＰパケット群内に存在するか否か調べ、存在する場合には、先に抽出したＳＹＮ用ＩＰパケットを含めてそれらのＳＹＮ用ＩＰパケットの個数をカウントする。さらに、そのカウントしたそれぞれのＳＹＮ用ＩＰパケットに対して、それぞれに対応するＡＣＫ用ＩＰパケット（詳しくは該ＳＹＮ用ＩＰパケットと同一の送信元ＩＰアドレスを有し、且つ、該ＳＹＮ用ＩＰパケットのＴＣＰヘッダ中のシーケンス番号の次のシーケンス番号を有するＡＣＫ用ＩＰパケット）であって、且つ該ＳＹＮ用ＩＰパケットの取得時刻から上記所定時間（２秒間）内に取得されたものが、同じ宛先ＩＰアドレスのＩＰパケット群内に存在するか否かを調べ、存在する場合には、その都度、上記のカウント数を「１」づつ減少させる。そして、最終的に、対応するＡＣＫ用ＩＰパケットの存在を調べ終わったときに上記のカウント数が所定数（例えば１６個）以上である場合には、ＳＹＮ　ＦＬＯＯＤの攻撃がなされていることを検知し、そのことを

示すデータと、この攻撃が検知されたＳＹＮ用ＩＰパケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データとを（以下、これらのデータを第２種攻撃検知データという）前記ディレクタ６に与える。このような処理が宛先ＩＰアドレスが同一で、且つ該宛先ＩＰアドレスがＬＡＮ１に属する全てのＩＰパケット群に対して順次行われる。なお、本実施形態では、ＳＹＮ用ＩＰパケットの個数に基づいてＳＹＮ　ＦＬＯＯＤを検知したが、次のような処理によりＳＹＮ　ＦＬＯＯＤを検知するようにしてもよい。すなわち、送信元ＩＰアドレスが同一で且つ、該送信元ＩＰアドレスがＬＡＮ１に属する各ＩＰパケット群に対し、該ＩＰパケット群に含まれるＳＹＮ／ＡＣＫ用ＩＰパケットをその取得時刻順に順次抽出する。そして、抽出した各ＳＹＮ／ＡＣＫ用ＩＰパケットの取得時刻から所定時間（例えば２秒間）内に取得されたＳＹＮ／ＡＣＫ用ＩＰパケットが、同じ送信元ＩＰアドレスのＩＰパケット群内に存在するか否か調べ、存在する場合には、先に抽出したＳＹＮ／ＡＣＫ用ＩＰパケットを含めてそれらのＳＹＮ／ＡＣＫ用ＩＰパケットの個数をカウントする。さらに、そのカウントしたそれぞれのＳＹＮ／ＡＣＫ用ＩＰパケットに対して、該ＳＹＮ／ＡＣＫ用ＩＰパケットの送信元ＩＰアドレスと同一の宛先ＩＰアドレスのＩＰパケット群を調べ、該ＳＹＮ／ＡＣＫ用ＩＰパケットに対応するＡＣＫ用ＩＰパケット（詳しくは該ＳＹＮ／ＡＣＫ用ＩＰパケットの送信元ＩＰアドレスと同一の宛先ＩＰアドレスを有し、且つ、該ＳＹＮ／ＡＣＫ用ＩＰパケットのＴＣＰヘッダ中のシーケンス番号の次のＡＣＫ番号を有するＡＣＫ用ＩＰパケット）であって、且つ該ＳＹＮ／ＡＣＫ用ＩＰパケットの取得時刻から上記所定時間（２秒間）内に取得されたものが、当該ＩＰパケット群内に存在するか否かを調べる。そして、そのようなＡＣＫ用パケットが存在する場合には、その都度、上記のカウント数を「１」づつ減少させる。そして、最終的に、対応するＡＣＫ用ＩＰパケットの存在を調べ終わったときに上記のカウント数が所定数（例えば１６個）以上である場合には、ＳＹＮ　ＦＬＯＯＤの攻撃がなされていることを検知する。なお、この場合にセンサ５からディレクタ６に与えるデータは、ＳＹＮ　ＦＬＯＯＤの攻撃を検知した示すデータと、上記ＳＹＮ／ＡＣＫ用ＩＰパケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データである。この場合、ＳＹＮ／ＡＣＫ用ＩＰパケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データは、それぞれ、先に説明した前記第２種攻撃検知データにおけるＳＹＮ用ＩＰパケット宛先ＩＰアドレスの値データ、送信元ＩＰアドレスの値データに相当するものである。一方、センサ５から前述のような第２種攻撃検知データを与えられた前記ディレクタ６は、該第２種攻撃検知データに含まれる送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば２分間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。同時に、ディレクタ６は、第２種攻撃検知データに含まれる宛先ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば２秒間）阻止するようにファイヤウォール２のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール２は、上記送信元ＩＰアドレスを有するＩＰパケット、あるいは上記宛先ＩＰアドレスを有するＩＰパケットがインターネット３から送信されてくると、そのＩＰパケットを廃棄し、ＬＡＮ１への進入を阻止する。これにより、ＳＹＮ　ＦＬＯＯＤの攻撃からＬＡＮ１が保護されると共に、この攻撃の対象とされていたＩＰアドレスのホストがダウンせずに正常状態に復帰することができる。なお、ポートスキャンの検知時の場合と同様、ディレクタ６は、第２種攻撃検知データにおける送信元ＩＰアドレスを有するＩＰパケットの排除に係る上記所定時間（２分間）が経過するまでの間に、先に与えられた第２種攻撃検知データと同一の第２種攻撃検知データがセンサ５から再度与えられれば、その時点から上記所定時間（２分間）、該第２種攻撃検知データの送信元ＩＰアドレスからのＩＰパケットのＬＡＮ１への進入を阻止するようにファイヤウォール２を制御する。このことは、第２種攻撃検知データにおける宛先ＩＰアドレスを有するＩＰパケットの排除についても同様である。従って、ＳＹＮ　ＦＬＯＯＤの攻撃が続いている限り、その攻撃に係る送信元ＩＰアドレスからのＩＰパケット、あるいはその攻撃に係る宛先ＩＰアドレスへのＩＰパケットは、ＬＡＮ１に進入することはできない。そして、ディレクタ６は、第２種攻撃検知データにおける送信元ＩＰアドレスを有するＩＰパケットの排除と、第２種攻撃検知データにおける宛先ＩＰアドレスを有するＩＰパケットの排除とのいずれについても、それぞれに対応する上記所定時間（２分間、２秒間）が経過するまでに、前記第２種攻撃検知データが与えられなかった場合には、その第２種攻撃検知データの送信元ＩＰアドレスを有するＩＰパケット、あるいは、第２種攻撃検知データの宛先ＩＰアドレスを有するＩＰパケットのＬＡＮ１への進入の阻止を解除する。前述のようにＳＹＮ　ＦＬＯＯＤの攻撃の検知処理を行ったセンサ５は、次に、第３の種類の攻撃（Ｔｅａｒｄｒｏｐ）の検知処理を行う。この処理では、センサ５は、宛先ＩＰアドレスが同一であるＩＰパケット群のうち、ＬＡＮ１に属する宛先ＩＰアドレスの各ＩＰパケット群に対し、該ＩＰパケット群に含まれる分轄されたＩＰパケット（以下、単に、分轄パケットという）を順次抽出する。この場合、ＩＰでは、分轄パケットは、そのＩＰヘッダ中の特定のフラグが「１」となっているか、もしくは、フラグメントオフセットといわれるデータが「０」より大きな値となっており、これに

より、分轄パケットを見出すことができる。そして、センサ５は、抽出した各分轄パケットの取得時刻から所定時間（例えば５分間）内に取得され、且つ、該分轄パケットとＩＰヘッダ中のＩＰ識別番号及びフラグメントオフセットの値がそれぞれ同一であるもの（抽出した分轄パケットと同一の分轄パケット）が、該分轄パケットと同じＩＰパケット群内にあるかを調べる。このとき、そのような分轄パケットがある場合には、先に抽出した分轄パケットを含めてそれらの分轄パケットの個数をカウントする。そして、このカウント数が所定数（例えば８０個）以上である場合には、Ｔｅａｒｄｒｏｐの攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知された分轄パケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データとを（以下、これらのデータを第３種攻撃検知データという）前記ディレクタ６に与える。このような処理が宛先ＩＰアドレスが同一で、且つ該宛先ＩＰアドレスがＬＡＮ１に属する全てのＩＰパケット群に対して順次行われる。一方、センサ５から前述のような第３種攻撃検知データを与えられた前記ディレクタ６は、前記ＳＹＮ　ＦＬＯＯＤが検知された場合と全く同じやり方で、ファイヤーウォール制御する。すなわち、第３種攻撃検知データに含まれる送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（２分間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。同時に、第３種攻撃検知データに含まれる宛先ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（２秒間）阻止するようにファイヤウォール２のフィルタ設定ファイルを書き換える。これにより、Ｔｅａｒｄｒｏｐの攻撃からＬＡＮ１が保護されると共に、この攻撃の対象とされていたＩＰアドレスのホストがダウンせずに正常状態に復帰することができる。上記のようにＴｅａｒｄｒｏｐの攻撃の検知処理を行ったセンサ５は、次に、第４の種類の攻撃（ＬＡＮＤ）の検知処理を行う。この処理では、センサ５は、宛先ＩＰアドレスが同一であるＩＰパケット群のうち、ＬＡＮ１に属する宛先ＩＰアドレスの各ＩＰパケット群から、該ＩＰパケット群の宛先ＩＰアドレスと同じ値の送信元ＩＰアドレスを有するＩＰパケットを抽出する。さらに、その抽出したＩＰパケットと同じ宛先ＩＰアドレスのＩＰパケット群の中から、該ＩＰパケットと同じ送信元ＩＰアドレスを有し、且つ該ＩＰパケットの取得時刻から所定時間（例えば２分間）内に取得されたＩＰパケットが存在するか否かを調べる。そして、そのようなＩＰパケットが存在する場合には、先に抽出したＩＰパケットを含めてそれらのＩＰパケットの該ＩＰパケットの個数をカウントする。このとき、該カウント数が所定数（例えば６個）以上である場合には、ＬＡＮＤの攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知されたＩＰパケットの送信元ＩＰアドレスの値データを（以下、これらのデータを第４種攻撃検知データという）前記ディレクタ６に与える。このような処理が宛先ＩＰアドレスが同一で、且つ該宛先ＩＰアドレスがＬＡＮ１に属する全てのＩＰパケット群に対して順次行われる。一方、センサ５から前述のような第４種攻撃検知データを与えられた前記ディレクタ６は、第４種攻撃検知データに含まれる送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有し、且つ、該送信元ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば５分間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール２は、上記送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットがインターネット３から送信されてくると、そのＩＰパケットを廃棄し、ＬＡＮ１への進入を阻止する。これにより、ＬＡＮＤの攻撃からＬＡＮ１が保護される。この場合、ポートスキャンの検知時の場合と同様、ディレクタ６は、第４種攻撃検知データにおける送信元ＩＰアドレスと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットの排除に係る上記所定時間（５分間）が経過するまでの間に、先に与えられた第４種攻撃検知データと同一の第４種攻撃検知データがセンサ５から再度与えられれば、その時点から上記所定時間（５分間）、該第４種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットのＬＡＮ１への進入を阻止するようにファイヤウォール２を制御する。従って、ＬＡＮＤの攻撃が続いている限り、その攻撃に係る送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットは、ＬＡＮ１に進入することはできない。そして、ディレクタ６は、上記所定時間（５分間）が経過するまでに、前記第４種攻撃検知データが与えられなかった場合には、その第４種攻撃検知データの送信元ＩＰアドレスと同一の送信元ＩＰアドレス及び宛先ＩＰアドレス有するＩＰパケットのＬＡＮ１への進入の阻止を解除する。

【０００９】なお、本実施形態では、第４種攻撃検知データとして、ＬＡＮＤの攻撃に係るＩＰパケットの送信元ＩＰアドレスの値データをディレクタ６に与えるようにしたが、ＬＡＮＤの攻撃に係るＩＰパケットの送信元ＩＰアドレスと、宛先ＩＰアドレスとは同じ値であるので、その送信元ＩＰアドレスの値データの代わりに、宛先ＩＰアドレスの値をディレクタ６に与えてもよいことはもちろんである。前述のように、ＬＡＮＤの攻撃の検知処理を行ったセンサ５は、次に第５の種類の攻撃（パスワードの獲得）を検知する処理を行う。この処理では、センサ５は、宛先ＩＰアドレスが同一であるＩＰパケット群のうち、ＬＡＮ１に属する宛先ＩＰアドレスの各ＩＰパケット群に対し、ＬＡＮ１のホストのユーザ名データ及びパスワードデータを含むＩＰパケットを抽出

する。それらの抽出したＩＰパケットの中から、ユーザ名データが同一で、且つ、パスワードデータが互いに異なり、且つ、連続した所定時間（例えば２分間）内に取得されたＩＰパケットの個数をカウントする。このとき、このカウント数が所定数（例えば２０個）以上であれば、クラッカーがパスワードを獲得するための第５の種類の攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知されたＩＰパケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データとを（以下、これらのデータを第５種攻撃検知データという）前記ディレクタ６に与える。このような処理が宛先ＩＰアドレスが同一で、且つ該宛先ＩＰアドレスがＬＡＮ１に属する全てのＩＰパケット群に対して順次行われる。一方、センサ５から前述のような第５種攻撃検知データを与えられた前記ディレクタ６は、該第５種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスとそれぞれ同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば１時間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール２は、上記送信元ＩＰアドレス及びＩＰアドレスを有するＩＰパケットがインターネット３から送信されてくると、そのＩＰパケットを廃棄し、ＬＡＮ１への進入を阻止する。これにより、パスワードの獲得を狙った第５の種類の攻撃からＬＡＮ１が保護される。なお、ポートスキャンの検知時の場合と同様、ディレクタ６は、第５種攻撃検知データにおける送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットの排除に係る上記所定時間（１時間）が経過するまでの間に、先に与えられた第５種攻撃検知データと同一の第５種攻撃検知データがセンサ５から再度与えられれば、その時点から上記所定時間（１時間）、該第５種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットのＬＡＮ１への進入を阻止するようにファイヤウォール２を制御する。従って、第５の種類の攻撃が続いている限り、その攻撃に係る送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットは、ＬＡＮ１に進入することはできない。そして、ディレクタ６は、上記所定時間（１時間）が経過するまでに、前記第５種攻撃検知データが与えられなかった場合には、その第５種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットＩＰパケットのＬＡＮ１への進入の阻止を解除する。前述のように、ＬＡＮＤの攻撃の検知処理を行ったセンサ５は、次に第６の種類の攻撃（スルーホールの攻撃）を検知する処理を行う。この処理では、センサ５は、宛先ＩＰアドレスが同一であるＩＰパケット群のうち、ＬＡＮ１に属する宛先ＩＰアドレスの各ＩＰパケット群に対し、例えばプリンタの論理名である「ｌｐｒ」というコマンドを有し、且つ、データサイズが１２８文字以上であるＩＰパケットを検索する。そして、そのようなＩＰパケットが見つかった場合には、ＬＡＮ１のホストのスルーホールを攻撃する第６の種類の攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知されたＩＰパケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データとを（以下、これらのデータを第６種攻撃検知データという）前記ディレクタ６に与える。一方、センサ５から前述のような第６種攻撃検知データを与えられた前記ディレクタ６は、該第６種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスとそれぞれ同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば６時間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール２は、上記送信元ＩＰアドレス及びＩＰアドレスを有するＩＰパケットがインターネット３から送信されてくると、そのＩＰパケットを廃棄し、ＬＡＮ１への進入を阻止する。これにより、ＬＡＮ１のホストのスルーホールを攻撃する第６の種類の攻撃からＬＡＮ１が保護される。なお、ポートスキャンの検知時の場合と同様、ディレクタ６は、第６種攻撃検知データにおける送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットの排除に係る上記所定時間（６時間）が経過するまでの間に、先に与えられた第６種攻撃検知データと同一の第５種攻撃検知データがセンサ５から再度与えられれば、その時点から上記所定時間（６時間）、該第６種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットのＬＡＮ１への進入を阻止するようにファイヤウォール２を制御する。従って、第６の種類の攻撃が続いている限り、その攻撃に係る送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットは、ＬＡＮ１に進入することはできない。そして、ディレクタ６は、上記所定時間（６時間）が経過するまでに、前記第６種攻撃検知データが与えられなかった場合には、その第５種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットＩＰパケットのＬＡＮ１への進入の阻止を解除する。以上説明したようにして、本実施形態のシステムによれば、センサ５や、ディレクタ６を導入するだけで、クラッカーによるＬＡＮ１への各種の攻撃をリアルタイムで検知しつつ、検知された攻撃からＬＡＮ１を保護する適正な処置を自動的に迅速に施すことができる。このため、ネットワーク管理者等は、クラッカーによる攻撃を考慮してＬＡＮ１を構築したり、頻繁にログファイルを参照したりする労力が大幅に削減され、ひいては、ＬＡＮ１の維持管理のコストを低減することができる。また、クラッカーによる各種攻撃をリアルタイムで検知できることから、攻撃が検知されない状況では、ＬＡＮ１と外部との通信を格別に制限する必要性が少なくなる。このため、通常時は、ＬＡＮ１の通信の自由度

を高めることができ、インターネット３上の情報資源を有用に活用することができる。なお、以上説明した実施形態では、ＬＡＮ１の入り口にファイヤウォール３を設けておき、クラッカーによる攻撃が検知されてとき、該ファイヤウォール３を制御することで、検知された攻撃を自動的に排除する処置を行ったが、クラッカーによる攻撃が検知されたときに、単に、その旨の報知をネットワーク管理者や、専門の警備管理者等に行うようにしてもよい。この場合には、例えば前記ディレクタ６あるいはセンサ５を公衆回線や専用回線を介してネットワーク管理者や、警備管理者等のホストに接続しておく。そして、攻撃が検知された場合に、前述した第１乃至第６種攻撃検知データのような情報をネットワーク管理者や警備管理者等のホストにディレクタ６あるいはセンサ５から＊ら送信する。このようにしたときには、検知された攻撃からＬＡＮ１を保護するための具体的な処置は、ネットワーク管理者等が直接的に行うこととなる。しかるに、この場合であっても、ネットワーク管理者等は、上記の報知を受けたときに処置を施せばよく、しかも攻撃の種類は検知されるので、攻撃に対する処置を比較的容易に施すことができる。

【図面の簡単な説明】

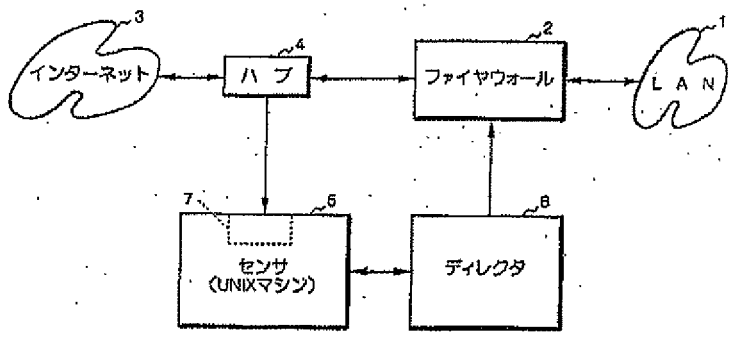
【図１】本発明のクラッカー監視システムの一実施形態のシステム構成図。

【符号の説明】

１…ＬＡＮ（ネットワーク）、２…ファイヤウォール（パケットフィルタ）、５…センサ（攻撃検知手段）、６…ディレクタ（処理手段）。

【図１】

〔図１〕



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　12/56			